

HP Docket No. 10007237-1

REMARKS

Applicants appreciate the Office's review of the present application. In response to the Office Action, the cited references have been reviewed, and the rejections and objections made to the claims by the Examiner have been considered. The claims presently on file in the present application are believed to be patentably distinguishable over the cited references, and therefore allowance of these claims is earnestly solicited.

In order to render the claims more clear and definite, and to emphasize the patentable novelty thereof, claims 1, 15, 21, 27, 37, 44, 49-51, 54-56, 58, 60, and 62-63 have been amended, claims 26 and 57 have been cancelled without prejudice, and new claims 64-70 have been added.

Support for any claim amendments and new claims is found in the specification, claims, and drawings as originally filed, and no new matter has been added. Accordingly, all claims presently on file in the subject application are in condition for immediate allowance, and such action is respectfully requested.

Rejections**Rejection Under 35USC §101**

Claims 1-12, 14-15, and 62-63 have been rejected under 35 USC §101 as directed to non-statutory subject matter. The Office states that these claims are "directed merely to an arrangement of data, which is non-functional descriptive material, and therefore is not statutory subject matter even though stored on a computer readable medium" (Office Action, p.4). Applicants respectfully disagree.

Non-functional descriptive material is defined as "certain types of descriptive material, such as music, literature, art, photographs, and mere arrangements or compilations of facts or data, without any functional interrelationship" (MPEP 2106.01 II).

Conversely, "'functional descriptive material' consists of data structures and computer

HP Docket No. 10007237-1

programs which impart functionality when employed as a computer component. (The definition of 'data structure' is 'a physical or logical relationship among data elements, designed to support specific data manipulation functions'...) ... "When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized" (MPEP 2106.01).

The Office takes the position that the descriptive matter of these claims is non-functional, stating that "the claim language does not explicitly encompass any specific function, rather, the claim is still only directed to a digital file and a digital string embedded in that file" (Office Action, p.3). Applicants disagree. The function performed by the computer processing the data structure stored on the medium using the key is to reveal in clear form the digital string having value to the purchaser that has been embedded in the preexisting digital file in a hidden manner. Because the digital string, such as the credit card number of the purchaser, can be revealed in this way to others who have access to the data structure, the purchaser will be reluctant to distribute the data structure to others. Such a function would be extremely useful to protect content such as, for example, digital music files and digital video files. As such, this constitutes a useful, concrete, and tangible result when used in a computer system.

The Office also states that "it does not appear that the claimed 'data structure' actually meets the definition of a data structure as ... 'a physical or logical relationship among data elements, designed to support specific data manipulation functions'" ... There is no specific data manipulation function that the file with the embedded string ... supports" (Office Action, p.3). Applicants again disagree. The data manipulation that the file supports is the extraction, using the key, of the hidden digital string from the file in clear form. The logical relationship between the key, the clear form of the digital string, the hidden form of the digital string, and the preexisting digital file supports this data manipulation function.

For at least these reasons, Applicants believe that the processor readable media of claims 1-12, 14-15, and 62-63 are clearly not "mere arrangements or compilations of facts or data,

HP Docket No. 10007237-1

without any functional interrelationship”, but rather are functional descriptive matter stored on a computer readable medium, and thus statutory. Accordingly, it is submitted that the rejection of these claims is improper and should be withdrawn.

Rejection Under 35 USC §112 Second Paragraph

Claims 1-12, 14, 27, 37, 47-55, 58, 60, and 63 have been rejected under 35 USC §112, paragraph 2, as being indefinite for failing to particularly point and distinctly claim the subject matter which the Applicant regards as the invention. In response, each of the Examiner's stated reasons have been addressed in the foregoing claim amendments and are briefly summarized below.

With regard to claims 1, 37, 50, 58, and 60, the Office states that the use of the term “only” is generally unclear. In response, claims 1 and 37 have been amended to delete “only”. Claims 50 and 60 have been amended to recite “a single one”. Claim 58 has been amended to recite “without using any said additional key”.

With regard to claim 49, the Office states that there is insufficient antecedent basis for “the encryption keys”. In response, claim 49 had been amended to depend from claim 22, which provides the necessary antecedent basis.

With regard to the rejection of claims 50 and 52-53 for insufficient antecedent basis, the above-described amendment to claim 49 provides the necessary antecedent basis.

With regard to claim 51, the Office states that there is insufficient antecedent basis for “said computer program”. In response, claim 51 had been amended to depend from claim 50, which provides the necessary antecedent basis.

With regard to claim 54, the Office states that there is insufficient antecedent basis for “the purchase of said valued content”, and there is no recitation of what information the purchaser is informed. In response, claim 54 had been amended to depend from claim 53, which provides the necessary antecedent basis.

With regard to claim 55, the Office states that there is insufficient antecedent basis for

HP Docket No. 10007237-1

"the encryption keys". In response, claim 55 had been amended to depend from claim 22, which provides the necessary antecedent basis.

With regard to claim 56, the Office states that there is insufficient antecedent basis for "said digital watermark". In response, claim 56 had been amended to depend from claim 25, which provides the necessary antecedent basis.

With regard to claim 58, the Office additionally states that the claim recites that the string can be recovered using only the two claimed keys, without using the encrypted string, which appears to be contradictory. Applicants note that the encrypted string is embedding in the decryption key, as disclosed in the specification generally at p.15, ln.17 – p.18, ln.4, and more particularly at, e.g., p.16, ln.19-22.

With regard to claim 63, the Office states that the limitation "at least some" renders the claim indefinite because "some" does not explicitly define a specific quantity or provide any basis for comparison as to how many "some" is intended to represent. Applicants disagree; this terminology is widely accepted in claims. However, to advance prosecution, claim 63 has been amended to recite "at least one".

Claims not referred to above have been rejected due to their dependence on a rejected base claim. Since the rejections of the base claims have been resolved as described heretofore, so are the rejections of their dependent claims.

In view of the foregoing, it is submitted that the rejections under 35 USC §112, paragraph 2, have been overcome and should be withdrawn.

Rejection Under 35USC §103

Claims 1-12, 14-15, 21-25, 27, 31-34, 37, 42-44, 47-56, and 59-63 have been rejected under 35 USC §103(a), as being unpatentable over U.S. patent 6,385,596 to Wiser et al. ("Wiser") in view of U.S. patent application publication 2001/0054081 to Fujiwara ("Fujiwara"), and further in view of U.S. patent 6,233,684 to Stefik et al. ("Stefik"). Applicants respectfully traverse the rejection, believe that the references in combination do not render the claims

HP Docket No. 10007237-1

obvious, and request reconsideration.

As to a rejection under §103(a), the U.S. Patent and Trademark Office ("USPTO") has the burden under §103 to establish a *prima facie* case of obviousness by showing some objective teaching in the prior art or generally available knowledge of one of ordinary skill in the art that would lead that individual to the claimed invention. See *In re Fine*, 837 F.2d 1071, 5 U.S.P.Q.2d 1596, 1598 (Fed. Cir. 1988). The Manual of Patent Examining Procedure (MPEP) section 2143 discusses the requirements of a *prima facie* case for obviousness. That section provides as follows:

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and reasonable expectation of success must be found in the prior art, and not based on applicant's disclosure.

More recently, the Supreme Court, quoting *In Re Kahn*, 441 F.3d, 977, 988 (CA Fed. 2006), has clarified that "[R]ejections on obviousness cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness" *Teleflex Inc. v. KSR Int'l Co.*, 82 USPQ2d 1385, 1396 (S.Ct. 2007).

The rejection of independent claim 1, and its dependent claims 2-12, 14, and 47-48, is respectfully traversed for at least the following reasons. Claim 1 recites:

"1. (Currently amended) A processor readable medium encoded with a data structure representing a valued content in a digital form, the data structure comprising:
a preexisting digital file having independent value to a provider; and
a digital string provided by a purchaser in clear form to a provider system of said preexisting digital file, said digital string having a latent value at least to said purchaser, said digital string modified according to a key and embedded two or more times in said preexisting

IIP Docket No. 10007237-1

digital file by said provider system, to form an embedded digital file, before the valued content is conveyed to said purchaser, wherein said digital string is embedded at least once in a hidden manner forming a hidden digital string, wherein said provider makes said key publicly available, and wherein said embedded digital file on said processor readable medium is processable by a computer program using said key to reveal said embedded digital string in clear form." (emphasis added)

The Office has not established a *prima facie* case of obviousness at least because the applied references do not teach or suggest all of Applicants' claim limitations.

The present application, as well as the cited references, is directed in part at protecting digital information from unauthorized or illicit use, typically by others who have not purchased or licensed the digital information. For this reason, a digital string that has latent value to a purchaser, such as his credit card information, is embedded in the digital information in a manner that is difficult to detect and/or remove. This serves as a disincentive for an authorized purchaser to distribute the digital information to an unauthorized other. One aspect of the present invention that is not taught or suggested by the cited references, however, is that the present invention (1) provides any member of the public the ability to obtain the legitimate user's credit card or other sensitive information from the digital information if the legitimate user distributes the digital information to others, and (2) notifies the public of a reward for doing so. (See specification, e.g. p.11, ln. 9-16; p.13, ln. 18 – p.14, ln. 5.)

In this regard, claim 1 recites that the embedded digital file is processable using the key which modified the digital string for embedding in the digital file to reveal the embedded digital string in clear form, and that this key is made publicly available by the provider.

The Office does not take the position that either the Wiser or Fujiwara reference discloses making the key publicly available or that the file can be processed using the key to reveal the string in clear form, and it is believed that neither reference discloses this. However, the Office states that "Stefik further discloses that the provider makes the key publicly available and that the file can be processed using the key to reveal the string in clear form (column 16, line 51 – column 18, line 5)" (Office Action, p.16). In addition, the Office further states that "Stefik

HP Docket No. 10007237-1

discloses the use of public keys used for retrieving the watermark (i.e. embedded) information (see Stefik, column 16, line 51 – column 18, line 5)” (Office Action, p.6). Applicants respectfully disagree.

The cited portion of the Stefik reference corresponds to Fig. 17, “a flowchart illustrating the steps involved in printing a digital work using the printer server implementation of Fig. 16” (col. 4, ln. 46-48). It is assumed, *arguendo*, that the digital string of claim 1 containing the purchaser’s information corresponds to the data embedded in the watermark of the Stefik reference.

First, within the trusted system environment of Fig. 16, the digital work, in the form of an encrypted document, does not contain any watermark, and thus does not include the digital string which is kept separately in certificates. Instead, the watermark is applied to the digital work only when it is printed:

“The distributor encrypts the document using DES or some other code, using a key length that is compatible with requirements of security and legal constraints, step 1702. It encrypts the document key in an envelope signed by the public key of server, step 1703. It sends the encrypted document to the server, step 1704. ... [T]he server stores the encrypted document, step 1705. At some point, the spooler gets ready to print the document. Before starting, it runs a process to create a new version of the glyph font that encodes the watermark data, step 1706. It looks up the required watermark information in its own certificates as well as certificates from the repository and user. Finally, the spooler begins imaging the document, one page at a time, step 1707.” (col. 17, ln. 14 – col. 18, ln. 5; emphasis added)

Thus the cited portion of the Stefik reference does not disclose processing the file (i.e. the encrypted document) using the key (i.e. the public key used to encrypt the document key) to reveal the digital string in clear form (i.e. by extracting it from the encrypted document). The encrypted document contains no such digital string. The Stefik reference, conversely, discloses almost the opposite - adding the watermark data to the document as it is printed (Fig. 17, step 1707, “Spooler images document with watermark”).

Second, there is no disclosure in the Stefik reference that the public key is used to modify the digital string (i.e. encode the watermark data), as recited in claim 1. Instead the public key is

HP Docket No. 10007237-1

disclosed as being used only to encrypt the document key that was utilized to encrypt the document. As discussed above, the document does not contain the digital string, which instead is kept in other certificates.

Therefore, for the reasons discussed herein, the applied references, alone or in combination, do not teach or suggest all of Applicants' claim limitations, and thus the rejection is improper at least for this reason and should be withdrawn.

Furthermore, the Office has not established a *prima facie* case of obviousness at least because there is no articulated reason with some rational underpinning that would have prompted a person of ordinary skill in the relevant field to combine the prior art elements in the manner claimed.

With regard to the combination of the Wiser and Fujiwara references, the Office articulates that the reason is "to effectively prevent illegal copying" (Office Action, p.16). Applicants respectfully disagree that this reason has sufficient rational underpinning to serve as a valid reason to combine. The whole purpose of the Wiser reference is precisely the same, to "provide for the secure delivery of audio data and related media, including text and images", which is "secure against unauthorized duplication by the user or by others" (Abstract; col. 2, ln. 4-6). There is no teaching or suggestion in the Wiser or Fujiwara reference that the techniques to provide security against unauthorized duplication of the Wiser reference are somehow ineffective. Nor does the Fujiwara reference assert that, or describe how, embedding the personal information of the purchaser in the media file itself, instead of in the media player passport required to play the media file as in Wiser, prevent illegal copying more effectively than Wiser does, so that it would be more effective than the Wiser reference.

Furthermore, considered as a whole, the illegal copying protection provided by the Fujiwara reference is far weaker, and far less effective, than the protection provided by the Wiser reference. For example, in the Wiser reference, the audio files are encrypted, and the keys are themselves protected by several layers of encryption. However, the Fujiwara reference only

HP Docket No. 10007237-1

provides rudimentary copy protection. In the Fujiwara reference, the personal data of the purchaser is added to the file header, and is displayed when the file is first accessed (para. [0049]). However, data file formats such as .pdf, .doc, .mp3, etc. are well known, and without applying any encryption, watermarking, steganographic effects, etc. to the data it would be easy to remove the personal information from the files. In addition, even if the password of the user could not be removed and thus would need to be disclosed to illicit users to access the file, the concern over sharing a personal password would be easily solved simply by the purchaser choosing some random password unrelated to any common passwords he uses.

Therefore, since the copy protection provided by the Fujiwara reference is far weaker than the copy protection provided by the Wiser reference, and since the Fujiwara reference does not disclose whether or why embedding the personal data of the purchaser in the file, instead of in the separate passport, would be more effective at preventing illegal copying, the reason provided by the Office to combine the references lacks the rational underpinning required for validly combining the references. Instead, the Office is using hindsight to pick and choose pieces from one reference or another and cobble them together based on the blueprint provided by Applicants' disclosure. Because the Office has not provided an articulated reason with some rational underpinning to combine the prior art elements in the manner claimed, it is improper to combine the Wiser and Fujiwara references, and the rejection under §103(a) should be withdrawn at least for this reason.

With regard to the combination of the Wiser and Stefik references, the Office articulates that the reason is "to increase robustness; that is, even if the visible string(s) is/are somehow removed, the invisible one(s) would remain and still allow control of the digital rights (see Stefik column 8, lines 55-56)" (Office Action, p.16). Applicants respectfully disagree that this reason has sufficient rational underpinning to serve as a valid reason to combine. The Wiser reference does not disclose using any visible strings that could be removed for the purchaser's personal, confidential information. Instead, the purchaser's personal information 414 (Fig. 4) is stored in encrypted form in passport 400. Furthermore, there is no suggestion in the Wiser reference that

HP Docket No. 10007237-1

such encrypted strings could be removed from the passport 400. Attempting to remove such strings, assuming they could even be located, would likely damage the passport 400 and thus prevent the audio in media data file 200 (Fig. 2) from being played.

For these reasons, the reason provided by the Office to combine the references lacks the rational underpinning required for validly combining the references. Instead, the Office is using hindsight to pick and choose pieces from one reference or another and cobble them together based on the blueprint provided by Applicants' disclosure. Because the Office has not provided an articulated reason with some rational underpinning to combine the prior art elements in the manner claimed, it is improper to combine the Wisner and Stefik references, and the rejection under §103(a) should be withdrawn at least for this reason.

Independent claims 37 and 62 (both currently amended) each recite limitations similar to those of claim 1, discussed above.

Claim 37 recites:

"37. (Currently amended) A system for generating valued content in a digital form by a provider, comprising:
a processor;
a storage device coupled to said processor;
an interface coupled to said processor and to a purchaser system; and
a valued content in a digital form comprising:
a preexisting digital file having independent value to a content owner, and
a digital string provided by a purchaser in clear form to said processor, said digital string having a latent value at least to said purchaser, modified according to a key and embedded two or more times in said preexisting digital file by said processor to form a second digital file to be conveyed to said purchaser system as valued content using said interface, wherein said provider makes said key publicly available, and wherein said embedded digital string is extractable in clear form from said second digital file using said key." (emphasis added)

Claim 62 recites:

"62. (Currently amended) A processor readable medium encoded with data representing a valued content and having a data structure comprising:
a preexisting digital file having independent value to a provider of said valued content;
two or more encoded digital strings embedded in said preexisting digital file by a

HP Docket No. 10007237-1

provider system, each encoded digital string generated using a key from an unencoded digital string provided by a purchaser to said provider system, said unencoded digital string having a latent value to at least said purchaser of said valued content;

wherein said key is made publicly available by said provider, and wherein said valued content is processable by a computer program using said key to reveal said unencoded digital string." (emphasis added)

For similar reasons as explained heretofore with regard to claim 1, the features of the present invention are not taught or suggested by the cited references in that at least the features by which a digital string that has latent value to a purchaser, embedded or encoded in a file, is revealed in clear form using a key made publicly available by the provider of the file, but no additional key, are neither taught nor suggested by the Wiser reference in combination with the Fujiwara and Stefik references.

Applicants respectfully traverse the Office's assertion that it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include the features recited in the claims of Applicants' invention. Such could be possible only in hindsight and in light of Applicants' teachings. Therefore, the rejection of independent claims 37 and 62, and their corresponding dependent claims 42-43 and 63, is improper at least for that reason and should be withdrawn.

The rejection of independent claim 21, and its dependent claims 22-25, 27, 31-34, and 49-56, is respectfully traversed for at least the following reasons. Claim 21 recites:

"21. (Currently amended) A method for protecting valued content comprising the steps of:

electronically acquiring by a provider a digital string from a purchaser to form an acquired digital string, said acquired digital string having a latent value at least to said purchaser;
modifying said acquired digital string in at least two different manners to form at least two different modified digital strings;

embedding said at least two different modified digital strings in a preexisting digital file to form an embedded digital file, said preexisting digital file having independent value to said provider;

embedding in said embedded digital file a provider digital string announcing a reward for detecting that said embedded digital file has been illicitly distributed to other than said purchaser;

HP Docket No. 10007237-1

and

conveying said embedded digital file, as valued content, to said purchaser.” (emphasis added)

The Office has not established a *prima facie* case of obviousness at least because the applied references do not teach or suggest all of Applicants’ claim limitations.

With regard to the limitation of embedding in the embedded digital file a provider digital string announcing a reward for detecting that said embedded digital file has been illicitly distributed to other than said purchaser, claim 21 was amended herein to include this limitation, which was previously recited in claim 26. In rejecting claim 26, the Office states

“Wiser, Fujiwara, and Stefik further disclose a provider string that can be encrypted (see Wiser, column 4, lines 1-4; column 7, lines 27-46; see also column 10, line 60 – column 11, line 7; Stefik column 3, lines 51-55).” (Office Action, p.20)

The Office does not state that such a string announces a reward for detecting that said embedded digital file has been illicitly distributed to other than said purchaser. To whatever extent, if any, that the cited portions of the Wiser and Stefik references may disclose a provider string that can be encrypted, neither the Wiser, Stefik, nor Fujiwara reference discloses that such a string announces a reward as recited in claim 21.

Therefore, for the reasons discussed herein, the applied references, alone or in combination, do not teach or suggest all of Applicants’ claim limitations, and thus the rejection is improper at least for this reason and should be withdrawn.

Furthermore, for similar reasons as has been explained heretofore with regard to claim 1, the Office has not established a *prima facie* case of obviousness at least because there is no suggestion or motivation to modify the reference or to combine reference teachings. Applicants respectfully traverse the Office’s assertion that it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include the features recited in the claims of Applicants’ invention. Such could be possible only in hindsight and in light of Applicants’ teachings. Therefore, the rejection is improper at least for this reason and should be withdrawn.

HP Docket No. 10007237-1

Independent claims 15 and 44 (both currently amended) each recite limitations similar to those of claim 21, discussed above.

Claim 15 recites:

"15. (Currently amended) A processor readable medium encoded with a data structure representing a valued content in a digital form, the data structure comprising:

a preexisting digital file having independent value to a provider; and

a digital string provided by a purchaser in clear form to a provider system of said preexisting digital file, said digital string encrypted by the digital processor of said provider system according to a key and combined with an encrypted provider digital string encrypted according to said key to form a combined encrypted digital string, said combined encrypted digital string embedded two or more times in said preexisting digital file by said provider system to form an embedded digital file before the valued content is conveyed to said purchaser, said digital string having a latent value at least to said purchaser which places said purchaser at increased financial risk when known by another, wherein said embedded digital file is processable by a computer program using said key to reveal said combined encrypted digital string in clear form, and wherein said encrypted provider digital string includes a notice of a reward for detecting that said valued content has been illicitly distributed to other than said purchaser." (emphasis added)

Claim 44 recites:

"44. (Currently amended) A system for generating valued content in a digital form comprising:

a purchaser processor adapted to communicate to a provider system an interest in purchasing a preexisting digital file from a content owner, said preexisting digital file having independent value to said content owner;

an interface coupled to said purchaser processor and said provider system, said provider system adapted to request a purchaser digital string from said purchaser processor, said purchaser digital string having a latent value at least to a purchaser;

a storage device coupled to said purchaser processor and adapted to send said purchaser digital string to said provider processor using said interface, wherein said provider system adds to said purchaser digital string a notice of a reward, modifies said purchaser digital string to form at least two different modified digital strings, and embeds said at least two different modified digital strings at least once each into said preexisting digital file to form a modified digital file, wherein the reward is for detecting that said modified digital file has been illicitly distributed to other than said purchaser." (emphasis added)

HP Docket No. 10007237-1

For similar reasons as explained heretofore with regard to claim 21, the features of the present invention are not taught or suggested by the cited references in that at least the features of a valued content file including an embedded or encoded provider string having a notice of a reward for detecting that the valued content file has been illicitly distributed to other than said purchaser are neither taught nor suggested by the Wiser reference in combination with the Fujiwara and Stefik references.

Applicants respectfully traverse the Office's assertion that it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include the features recited in the claims of Applicants' invention. Such could be possible only in hindsight and in light of Applicants' teachings. Therefore, the rejection of independent claims 15 and 44, and their corresponding dependent claims 59-61, is improper at least for that reason and should be withdrawn.

Dependent claim 3 is further patentably distinguishable over the cited references because claim 3 recites additional limitation neither taught nor suggested by the cited references in combination. In this regard, claim 3 recites:

"3. (Previously presented) A processor readable medium in accordance with claim 2, wherein said encrypted digital string further comprises a private digital string encrypted using a public key of a private/public encryption key pair and a public digital string encrypted using a private key of said private/public key encryption key pair." (emphasis added)

The Office states that "Wiser, Fujiwara, and Stefik further disclose that the string is encrypted using a private or public key (Wiser, column 9, lines 19-20; Stefik, column 16, line 51 – column 18, line 5)" (Office Action, p.16)

Applicants respectfully disagree. The cited portion of the Wiser reference teaches that

"The consumer private key 412 and personal information 414 are encrypted with a user's registration key 420. This key is also generated by the media licensing center 110. The registration key 420 is stored in the passport 400 encrypted using a passphrase entered by the user during the registration process" (col. 9, ln. 19-23).

The reference teaches nothing about the nature of the registration key 420 other than it is

HP Docket No. 10007237-1

strong and randomly generated (col. 13, ln. 50-51). The cited portion of the Stefik reference describes the steps involved in printing a digital work using a spooler 1603 coupled to a printer 1604. With regard to keys it discloses only that

“The distributor encrypts the document using DES or some other code, using a key length that is compatible with requirements of security and legal constraints, step 1702. It encrypts the document key in an envelope signed by the public key of server, step 1703.” (col. 16, ln. 66 – col. 17, ln. 4).

There is no teaching or suggesting that a public digital string is encrypted using a private key, and a private digital string encrypted using a public key (assuming, arguendo, that the document can be considered a private digital string). Nor do the Wiser nor Fujiwara references disclose such limitations.

Therefore, for the reasons discussed herein, the applied references, alone or in combination, do not teach or suggest all of Applicants’ claim limitations, and thus the rejection is improper at least for this additional reason and should be withdrawn.

Dependent claim 51 is further patentably distinguishable over the cited references because claim 51 recites additional limitation neither taught nor suggested by the cited references in combination. In this regard, claim 51 recites:

“51. (Currently amended) A method in accordance with the method of claim 50, wherein said computer program, or a process performable by said computer program to reveal said digital string, is made publicly available by said provider.” (emphasis added)

With regard to claim 51, the Office states only that “Wiser, Fujiwara, and Stefik further disclose that at least one key and a process to extract the key in clear form is made publicly available by the provider (column 16, line 51 – column 18, line 5)” (Office Action, p.21). Though not specified, Applicants assume that the Office is referring to the Stefik reference.

Applicants respectfully disagree. The cited portion of the Stefik reference describes the steps involved in printing a digital work using a spooler 1603 coupled to a printer 1604. Nothing in the cited portion, or in the steps of the flowchart of Fig. 17, discloses a computer program or a

HP Docket No. 10007237-1

process performable thereby which reveals a digital string from the embedded digital file representing valued content. Nor do the Wiser nor Fujiwara references.

Therefore, for the reasons discussed herein, the applied references, alone or in combination, do not teach or suggest all of Applicants' claim limitations, and thus the rejection is improper at least for this additional reason and should be withdrawn.

Dependent claim 53, and its sub-dependent claim 54, are further patentably distinguishable over the cited references because claim 53 recites additional limitation neither taught nor suggested by the cited references in combination. In this regard, claim 53 recites:

"53. (Previously presented) A method in accordance with the method of claim 49, wherein said provider informs said purchaser that said at least one of the encryption keys is made publicly available." (emphasis added)

With regard to claim 53, the Office states only that "Wiser, Fujiwara, and Stefik further disclose that at least one key and a process to extract the key in clear form is made publicly available by the provider (column 16, line 51 – column 18, line 5)" (Office Action, p.21). Though not specified, Applicants assume that the Office is referring to the Stefik reference.

Applicants respectfully disagree. The cited portion of the Stefik reference describes the steps involved in printing a digital work using a spooler 1603 coupled to a printer 1604. Nothing in the cited portion, or in the steps of the flowchart of Fig. 17, discloses that the provider informs the purchaser that at least one of the encryption keys is made publicly available. Furthermore, there would be no need for such to be done in a trusted rendering system where the digital file is securely maintained at all times, as taught by the Stefik reference (col. 4, lines 52-60).

Neither the Wiser nor the Fujiwara reference teach or suggest the limitations of claim 53.

Therefore, for the reasons discussed herein, the applied references, alone or in combination, do not teach or suggest all of Applicants' claim limitations, and thus the rejection is improper at least for this additional reason and should be withdrawn.

HP Docket No. 10007237-1

Dependent claim 55 is further patentably distinguishable over the cited references because claim 55 recites additional limitation neither taught nor suggested by the cited references in combination. In this regard, claim 55 recites:

“55. (Currently amended) A method in accordance with the method of claim 22, wherein at least one of the encryption keys is made publicly available by said provider at a first time, and wherein at least another one of the encryption keys is made publicly available by said provider at a second time later than the first time.” (emphasis added)

With regard to claim 55, the Office states only that “Wiser, Fujiwara, and Stefik further disclose that at least one key and a process to extract the key in clear form is made publicly available by the provider (column 16, line 51 – column 18, line 5)” (Office Action, p.21). Though not specified, Applicants assume that the Office is referring to the Stefik reference.

Applicants respectfully disagree. The cited portion of the Stefik reference describes the steps involved in printing a digital work using a spooler 1603 coupled to a printer 1604. Nothing in the cited portion, or in the steps of the flowchart of Fig. 17, discloses that the provider makes publicly available at least one of the encryption keys at a first time, and at least another one of the encryption keys at a second time later than the first time. Furthermore, there would be no need for such to be done in a trusted rendering system where the digital file is securely maintained at all times, as taught by the Stefik reference (col. 4, lines 52-60).

Neither the Wiser nor the Fujiwara reference teach or suggest the limitations of claim 55.

Therefore, for the reasons discussed herein, the applied references, alone or in combination, do not teach or suggest all of Applicants' claim limitations, and thus the rejection is improper at least for this additional reason and should be withdrawn.

Claims 36 and 58 have been rejected under 35 USC §103(a), as being unpatentable over U.S. patent 6,385,596 to Dwork et al. ("Dwork") in view of U.S. patent application publication 2001/0054081 to Fujiwara ("Fujiwara"), and further in view of U.S. patent 6,233,684 to Stefik et al. ("Stefik"). Applicants respectfully traverse the rejection, believe that the references in combination do not render the claims obvious, and request reconsideration.

HP Docket No. 10007237-1

The rejection of independent claim 36, and its dependent claim 58, is respectfully traversed for at least the following reasons. Claim 36 recites:

“36. (Previously presented) A method for a provider to protect valued content comprising the steps of:

electronically acquiring a digital string from a purchaser, said acquired digital string having a latent value at least to said purchaser;

encrypting said acquired digital string according to at least one first encryption key to form a corresponding at least one encrypted digital string;

embedding said at least one encrypted digital string in a decryption key;

embedding said acquired digital string two or more times in a preexisting digital file having independent value to a content owner to form an embedded digital file, wherein said acquired digital string is embedded at least once in a hidden manner;

encrypting said embedded digital file according to a second encryption key to form an encrypted digital file;

conveying said decryption key and said encrypted digital file, as valued content, to said purchaser; and

said provider conveying to the public a published one of said at least one first encryption key, the published encryption key usable to recover in clear form said acquired digital string from said decryption key.” (emphasis added)

The Office has not established a *prima facie* case of obviousness at least because the applied references do not teach or suggest all of Applicants’ claim limitations.

With regard to the limitation of the provider conveying to the public a published one of the first encryption keys which is usable to recover in clear form the digital string having latent value to the purchaser from said decryption key, the Office does not take the position that either the Dwork or Fujiwara reference discloses conveying a published one of the first encryption keys to the public, or that the decryption key can be processed using the published encryption key to reveal the string in clear form, and it is believed that neither reference discloses this. However, the Office states that “Stefik further discloses that the provider conveys a key to the public and that the file can be processed using the key to reveal the string in clear form (column 16, line 51 – column 18, line 5)” (Office Action, p.26). In addition, the Office further states that Stefik discloses “where public keys are used for retrieving the watermark, i.e. embedded, information” at col.16, ln. 51 – col.18, ln. 5)” (Office Action, p.10). Applicants respectfully disagree.

HP Docket No. 10007237-1

First, claim 36 recites that the acquired digital string is recovered in clear form from the decryption key. However, the Stefik reference “encrypts the document key in an envelope signed by the public key of server” (col.17, ln. 1-3; emphasis added). The digital string having latent value to the purchases (e.g. credit card information) is not stored in the document key of the Stefik reference, but rather in various certificates (col.18, ln. 1-3). Thus there is no disclosure that the digital string can be recovered from any decryption key.

Second, for similar reasons as have been discussed heretofore with regard to claim 1, the Stefik reference discloses that the digital watermark is generated only when the document is printed. Thus the public key and the document key, which are both generated in advance of printing the document, cannot contain the digital string, and thus it is not possible to recover the digital string from the public key of the server or from the document key.

Therefore, for the reasons discussed herein, the applied references, alone or in combination, do not teach or suggest all of Applicants’ claim limitations, and thus the rejection is improper at least for this reason and should be withdrawn.

Furthermore, the Office has not established a *prima facie* case of obviousness at least because there is no articulated reason with some rational underpinning that would have prompted a person of ordinary skill in the relevant field to combine the prior art elements in the manner claimed.

Applicants respectfully disagree that this reason has sufficient rational underpinning to serve as a valid reason to combine. The whole purpose of the Dwork reference is precisely the same, to provide “Method and System for Protection of Digital Information” to prevent “illegal copying and distribution” (Title; col. 1, ln. 62). There is no teaching or suggestion in the Dwork or Fujiwara reference that the techniques of the Dwork reference to protect against illegal copying are somehow ineffective. Nor does the Fujiwara reference assert that, or describe how, embedding the digital string containing the personal information of the purchaser in the content itself, instead of in the key, prevents illegal copying more effectively than Dwork does.

HP Docket No. 10007237-1

Furthermore, considered as a whole, the illegal copying protection provided by the Fujiwara reference is far weaker, and far less effective, than the protection provided by the Dwork reference. For example, the Dwork reference teaches the use of "an extremely long decryption key" with an extrication function that is "computationally infeasible to invert" (col. 4, ln. 5-9). However, the Fujiwara reference only provides rudimentary copy protection. In the Fujiwara reference, the personal data of the purchaser is added to the file header, and is displayed when the file is first accessed (para. [0049]). However, data file formats such as .pdf, .doc, .mp3, etc. are well known, and without applying any encryption, watermarking, steganographic effects, etc. to the data it would be easy to remove the personal information from the files. In addition, even if the password of the user could not be removed and thus would need to be disclosed to illicit users to access the file, the concern over sharing a personal password would be easily solved simply by the purchaser choosing some random password unrelated to any common passwords he uses.

Therefore, since the copy protection provided by the Fujiwara reference is far weaker than the copy protection provided by the Dwork reference, and since the Fujiwara reference does not disclose whether or why embedding the personal data of the purchaser in the content, instead of in the key, would be more effective at preventing illegal copying, the reason provided by the Office to combine the references lacks the rational underpinning required for validly combining the references. Instead, the Office is using hindsight to pick and choose pieces from one reference or another and cobble them together based on the blueprint provided by Applicants' disclosure.

In addition, the combination of the Dwork reference and the Fujiwara reference would be inoperative to produce the intended result of the Dwork reference. The Dwork reference discloses mass mailing of content on CD-ROMs, or mass distribution of content via the Internet, satellite, or cable TV (col. 7, ln. 22-37). However, such mass distribution of particular content file(s) would not be possible if each individual copy of the content file(s) had to be customized with "[t]he personal data of the requesting user ... embedded in the created copy to create the

HP Docket No. 10007237-1

delivery data contents” as taught by the Fujiwara reference (para. [0047]). Put another way, the Fujiwara reference teaches away from combination with the Dwork reference.

Because the Office has not provided an articulated reason with some rational underpinning to combine the prior art elements in the manner claimed, because the combination of the Dwork and Fujiwara references would be inoperative, and because the Fujiwara reference teaches away from combination with the Dwork reference, it is improper to combine the Wiser and Fujiwara references, and the rejection under §103(a) should be withdrawn at least for this reason.

With regard to the combination of the Dwork and Stefik references, the Office articulates that the reason is “to increase robustness; that is, even if the visible string(s) is/are somehow removed, the invisible one(s) would remain and still allow control of the digital rights (see Stefik column 8, lines 55-56)” (Office Action, p.26-27). Applicants respectfully disagree that this reason has sufficient rational underpinning to serve as a valid reason to combine. The Dwork reference does not disclose using any visible strings that could be removed for the purchaser’s personal, confidential information. Instead, user number n_i , which uniquely identifies and is valuable to the user, is stored in encrypted form in signet pair (a_i, n_i) with authorization number a_i . Furthermore, there is no suggestion in the Dwork reference that the encrypted user number could be removed from the encrypted signet pair. Attempting to remove such information, assuming it could even be located, would likely damage the signet pair and thus prevent the content from being accessed.

For these reasons, the reason provided by the Office to combine the references lacks the rational underpinning required for validly combining the references. Instead, the Office is using hindsight to pick and choose pieces from one reference or another and cobble them together based on the blueprint provided by Applicants’ disclosure. Because the Office has not provided an articulated reason with some rational underpinning to combine the prior art elements in the manner claimed, it is improper to combine the Dwork and Stefik references, and the rejection under §103(a) should be withdrawn at least for this reason.

HP Docket No. 10007237-1

New Claims

New claim 64 recites:

"64. (New) A method for protecting valued content comprising the steps of:
electronically acquiring by a provider a digital string from a purchaser to form an acquired digital string, said acquired digital string having a latent value at least to said purchaser;
modifying said acquired digital string in at least two different manners to form at least two different modified digital strings;
embedding said at least two different modified digital strings in a preexisting digital file to form an embedded digital file, said preexisting digital file having independent value to said provider;
embedding in said embedded digital file a provider digital string having information supplied by a provider; and
after embedding said modified digital strings and said provider digital string, conveying said embedded digital file, as valued content, to said purchaser." (emphasis added)

It is believed that claim 64 is allowable at least because none of the cited references, alone or in combination, teach or suggest that a provider string is embedded in a digital file prior to the conveyance of the file to a purchaser. In the Stefik reference, the watermark (which may, arguendo, include a provider string) is not embedded in a digital file. The watermark is applied only when the content is being rendered (e.g. a document printed, or a music file played). In the Stefik reference, rendering (arguendo, adding the watermark of the provider string) occurs after the digital file has been conveyed to the purchaser, whereas claim 64 requires that embedding the provider digital string be done before conveying the digital file to the purchaser. Furthermore, the Stefik reference does not teach or suggest that any complete digital file is ever generated as, c.g., an intermediate step of the output rendering process, because it discloses that the spooler images the document one page at a time (col. 18, lines 4-5).

New claim 65 recites:

"65. (New) A processor readable medium in accordance with claim 1, wherein said embedded digital file on said processor readable medium is processable by said computer program using said key but no additional key to reveal said embedded digital string in clear

HP Docket No. 10007237-1

form.” (emphasis added)

It is believed that claim 65 is allowable at least because none of the cited references, alone or in combination, teach or suggest that the embedded digital file is processable using the key, but no additional key to reveal said embedded digital string in clear form. In the Stefik reference, the key is disclosed as a “public key” used in trust boxes of the trust system of the Stefik reference. This refers to public key encryption, a technique in which an additional key, a corresponding private key, is needed to decrypt an encrypted message or document to reveal it in clear form. As such, this is contrary to the limitations of claim 65.

New claims 67, 69, and 70 recite similar limitations, and are believed allowable for similar reasons.

New claim 66 recites:

“66. (New) A processor readable medium in accordance with claim 1, wherein said embedded digital file on said processor readable medium is not processable by said computer program using said key to reveal said preexisting digital file in clear form.” (emphasis added)

It is believed that claim 66 is allowable at least because none of the cited references, alone or in combination, teach or suggest that the embedded digital file is not processable using said key to reveal said preexisting digital file in clear form. As explained heretofore with reference to claim 1, the public key of the Stefik reference is disclosed only as being used only to encrypt the document key that was utilized to encrypt the document.

New claim 68 recites similar limitations, and is believed allowable for similar reasons.

Conclusion

Attorney for Applicants has reviewed each one of the cited references made of record and not relied upon, and believes that the claims presently on file in the subject application patentably distinguish thereover, either taken alone or in combination with one another.

HP Docket No. 10007237-1

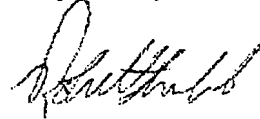
Therefore, all claims presently on file in the subject application are in condition for immediate allowance, and such action is respectfully requested. If it is felt for any reason that direct communication with Applicant's attorney would serve to advance prosecution of this case to finality, the Examiner is invited to call the undersigned Robert C. Sismilich, Esq. at the below-listed telephone number.

HP Docket No. 10007237-1

**AUTHORIZATION TO PAY AND PETITION
FOR THE ACCEPTANCE OF ANY NECESSARY FEES**

If any charges or fees must be paid in connection with the foregoing communication (including but not limited to the payment of an extension fee or issue fees), or if any overpayment is to be refunded in connection with the above-identified application, any such charges or fees, or any such overpayment, may be respectively paid out of, or into, the Deposit Account No. 08-2025 of Hewlett-Packard Company. If any such payment also requires Petition or Extension Request, please construe this authorization to pay as the necessary Petition or Request which is required to accompany the payment.

Respectfully submitted,



Robert C. Sismilich
Reg. No. 41,314
Attorney for Applicant(s)
Telephone: (941) 677-6015

Date: 11/23/07

Hewlett-Packard Company
Intellectual Property Administration
P. O. Box 272400
Fort Collins, CO 80527-2400